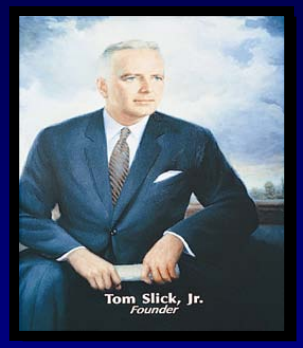
Smart Grid Embedded Cyber Security: Ensuring Security While Promoting Interoperability

Communications and Embedded Systems Department
Southwest Research Institute
Gary Ragsdale, Ph.D., P.E.
August 24 – 25, 2010

Proceedings of the 17th Symposium for
Improving Building Systems
in Hot and Humid Climates
Austin Texas
August 24-25, 2010

Southwest Research Institute

1947



- 60+ years, founded 1947
- 3200+ employees
- 4000+ R&D projects/yr.
- $500M revenue
- 1200 acres
- 170 buildings
- 2.1 million square feet

2009

Proceedings of the 17th Symposium for
Improving Building Systems
in Hot and Humid Climates
Austin Texas
August 24-25, 2010

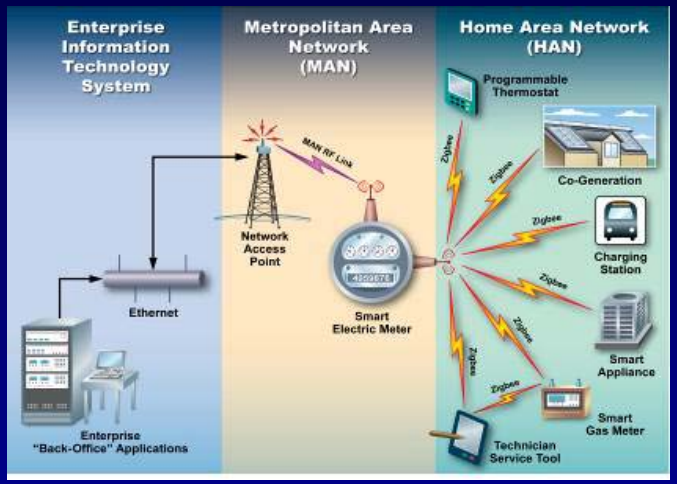
Presentation Objectives

- Report on the security posture of Smart Grid devices
- Describe progress made in Smart Grid security
- Propose a more robust approach to SG security
- Describe needs for further research and development

Proceedings of the 17th Symposium for
Improving Building Systems
in Hot and Humid Climates
Austin Texas
August 24-25, 2010

What is Smart Grid Infrastructure Assessment?

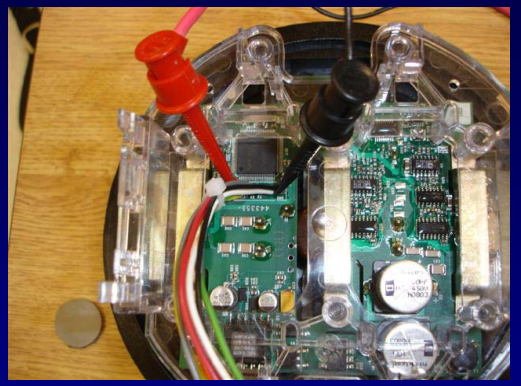
- Security analysis of smart grid systems & communications
  - Reverse engineering
  - Penetration testing
  - Threat and risk assessment

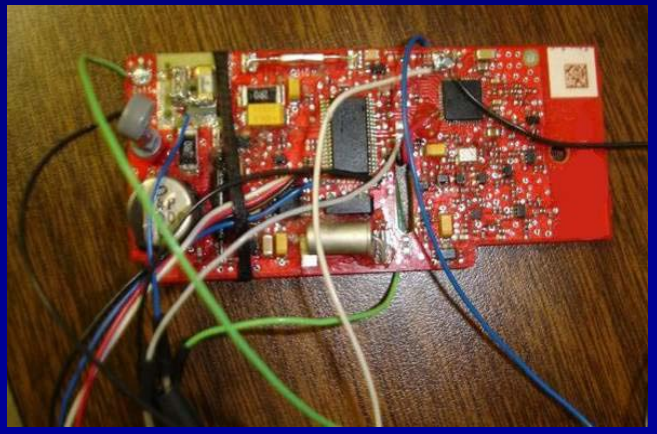


- Advanced security methods
  - Power analysis for key discovery
  - Hardware attacks such as "decapping" chips
  - Developing vulnerability exploits

Hacking Proprietary Smart Meters

- Recovery of crypto keys, security tokens, & passwords via physical attacks on hardware
- Firmware extraction through debug interfaces and monitoring of system state with In-Circuit Emulators (ICE)
- Firmware Analysis, Reverse Engineering, and Modification
- Physical Bus Snooping and Traffic Injection
- Traffic capture, spoofing, and denial of service attacks on radios





Proprietary SG Built with Off-the-Shelf Technology

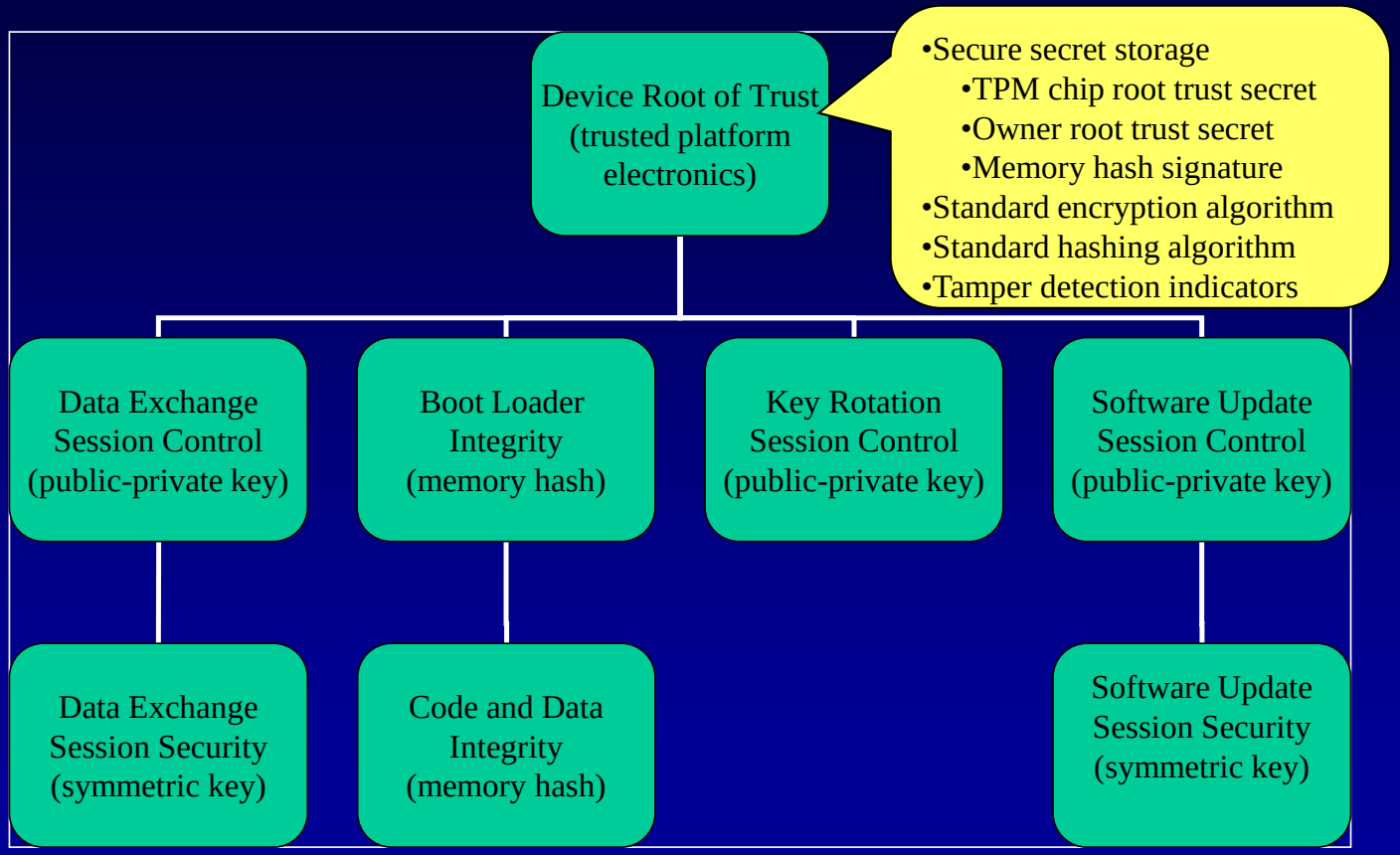
- Off-the-shelf microcontrollers
  - Reference electronics design kits
  - Chip specifications and application notes
  - Software development and debug tools
  - Programming and maintenance tools
- Off-the-shelf communications technology
  - Radio electronics & protocol kits & documentation
  - Software-defined radio development tools
  - Communication protocols simulators

Implementing TCG Standards Within Systems

- Trusted Platform Module (TPM)
  - Provides root of trust
  - Secure storage
  - Signing & hashing functions
  - Tamper detection
  - Accelerates cryptography
- TPM software stack
  - Implements TCG stack
  - Manages TPM chip

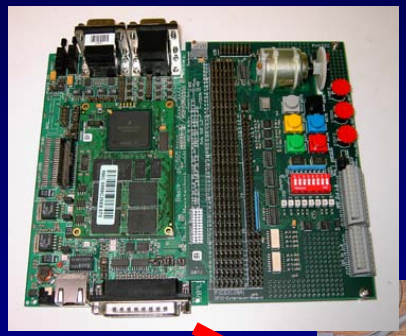
Trusted Platform Module Development Board with AT97SC3201 TPM Attached

Typical Trusted Computing Platform Trust Hierarchy

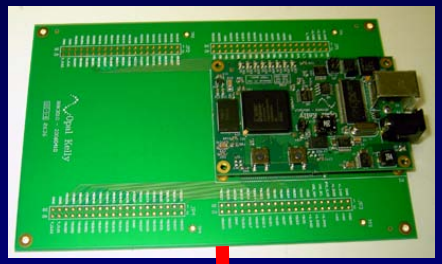


Prototypical SG Trusted Computing Platform

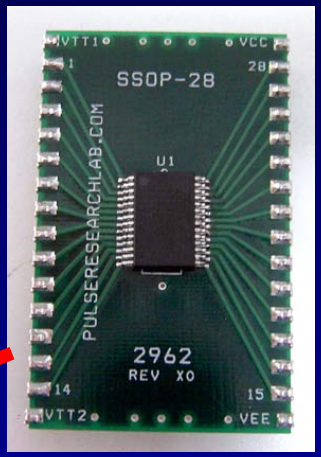
Phytec with Expansion Board

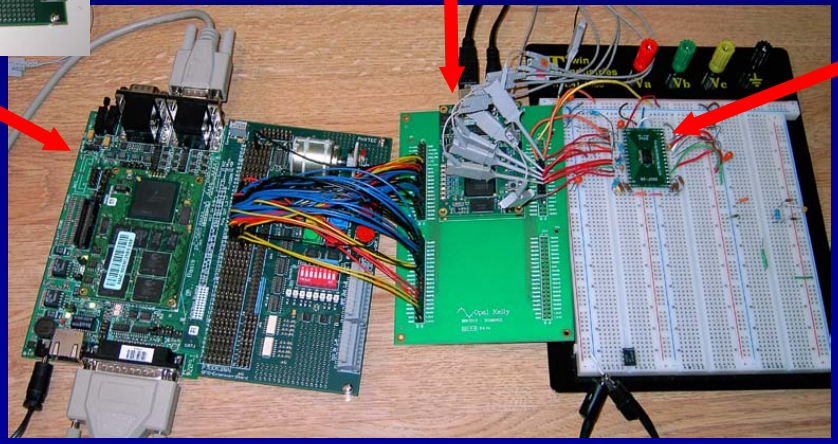


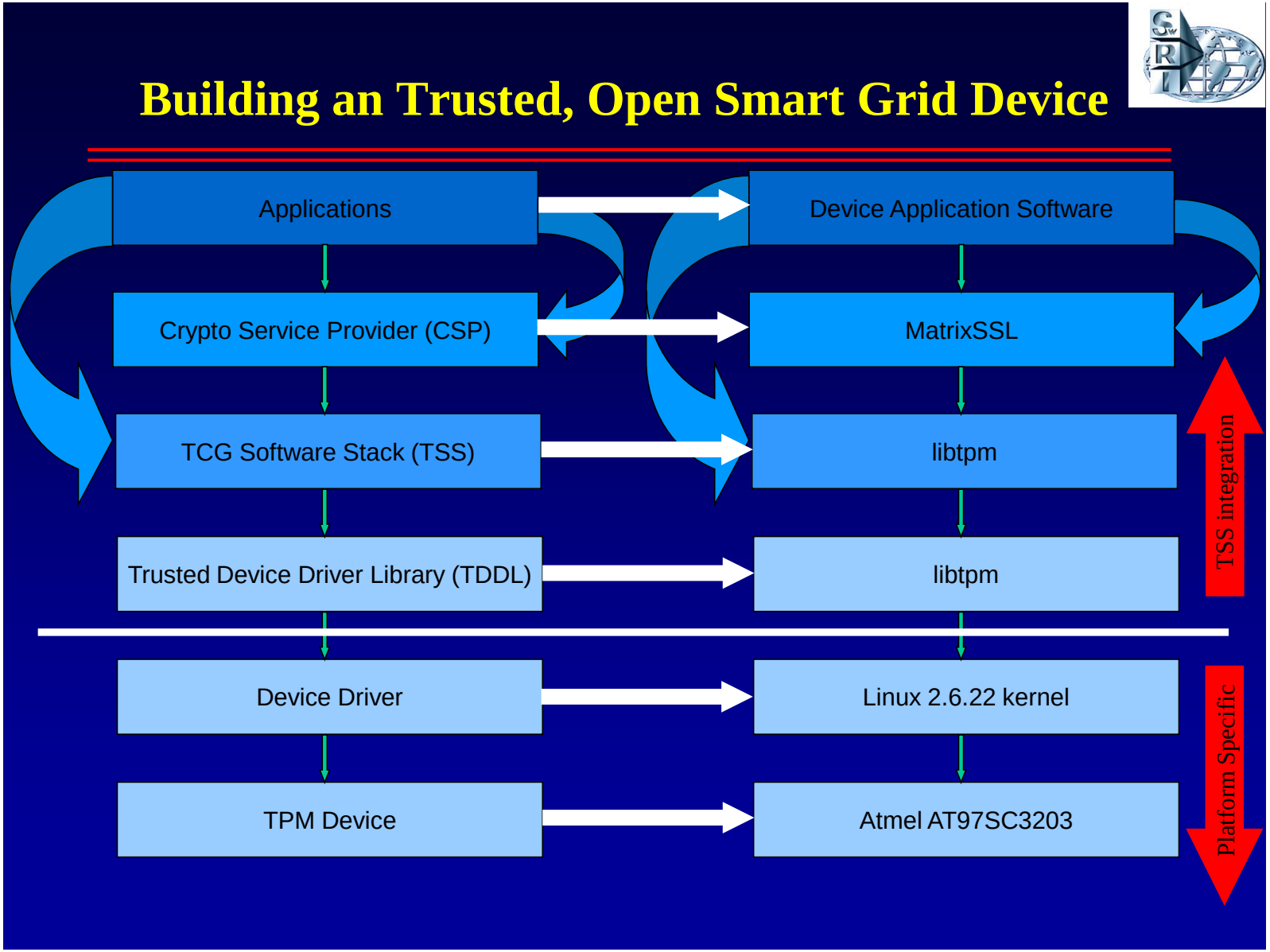
Opal Kelly FPGA with Expansion Board



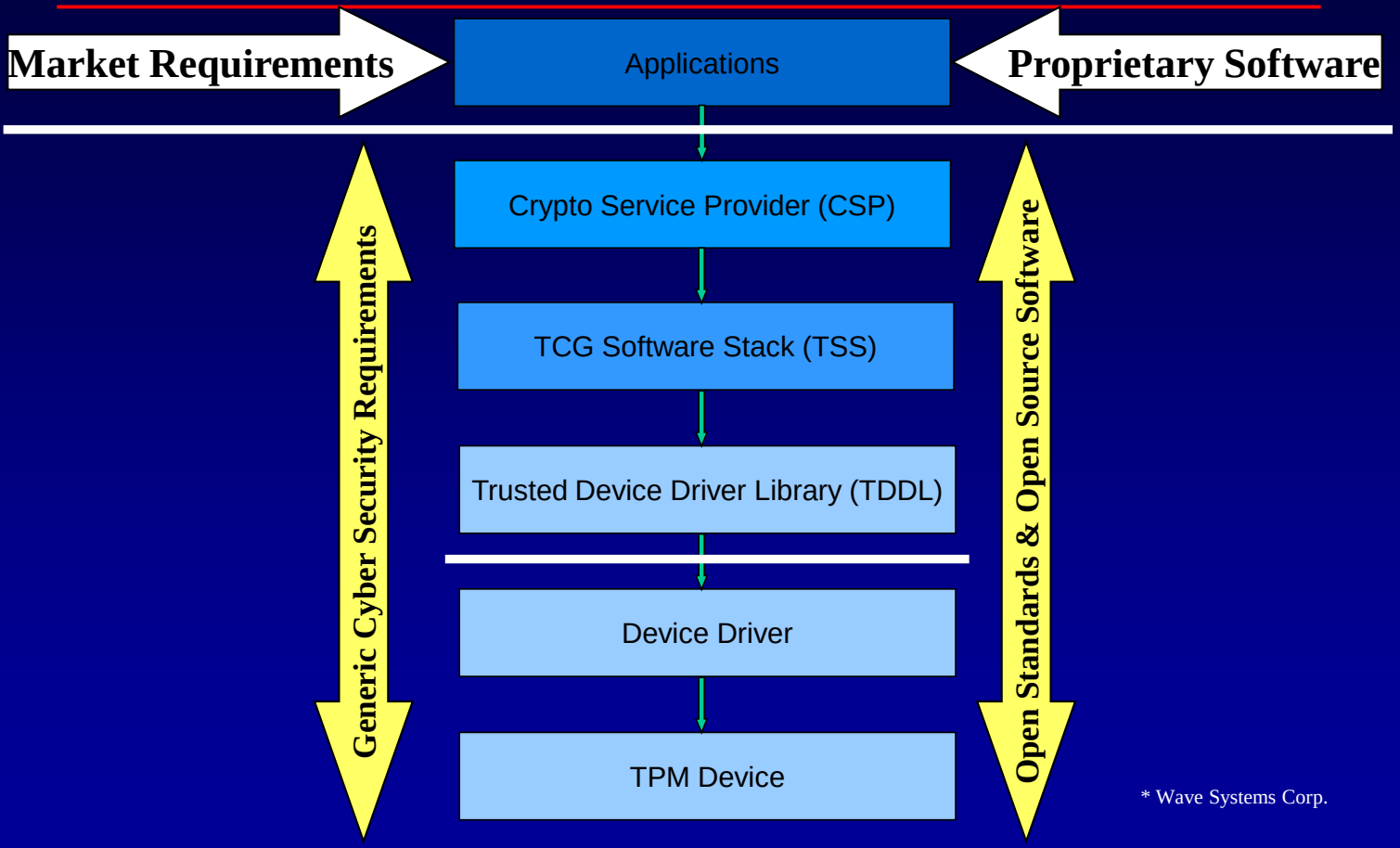
Atmel TPM chip mounted on prototyping board





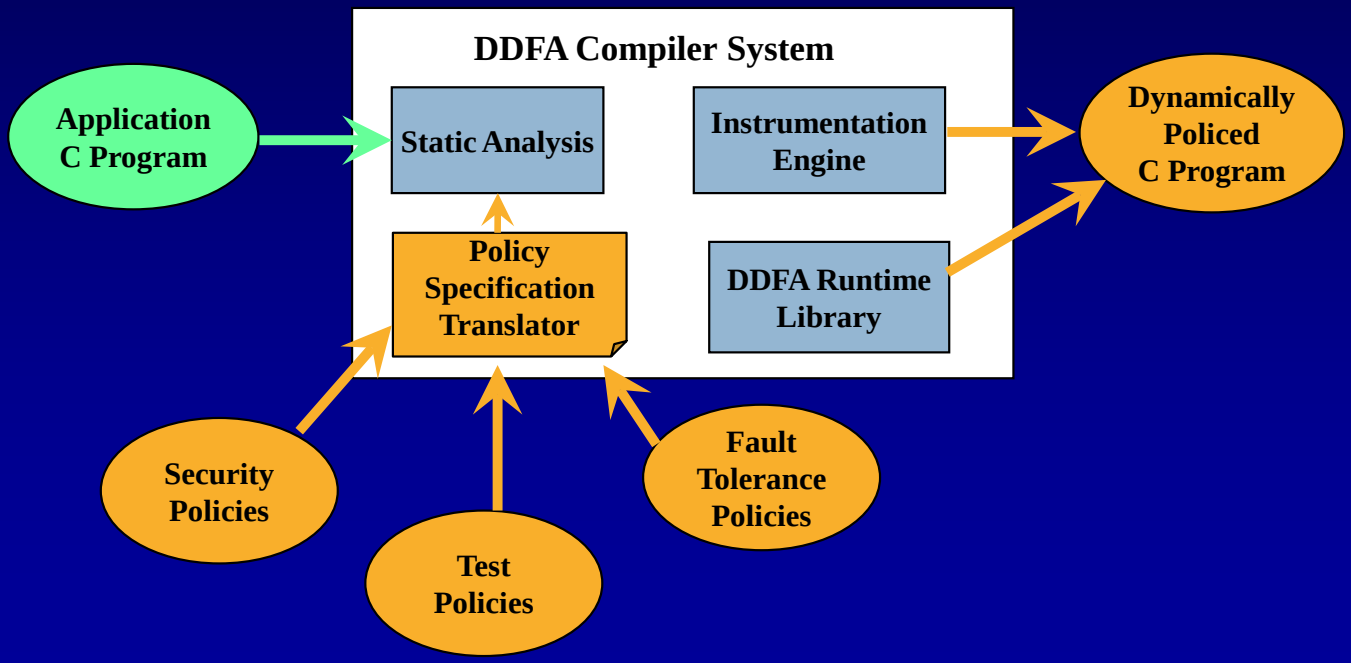

Building an Trusted, Open Smart Grid Device
Applications
Crypto Service Provider (CSP)
TCG Software Stack (TSS)
Trusted Device Driver Library (TDDL)
Device Driver
TPM Device
Device Application Software
MatrixSSL
libtpm
libtpm
Linux 2.6.22 kernel
Atmel AT97SC3203
TSS integration
Platform Specific

Building an Trusted, Open Smart Grid Device



* Wave Systems Corp.

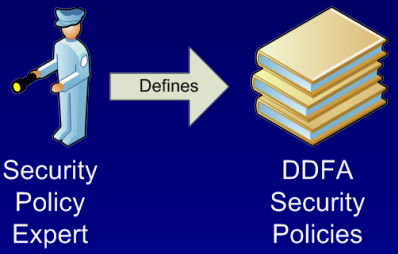
Dynamic Data Flow Analysis System Architecture

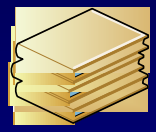


Development with DDFA

Runtime library provides the dynamic data flow analysis capability

Security policy separate from source code

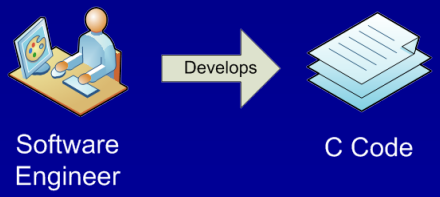


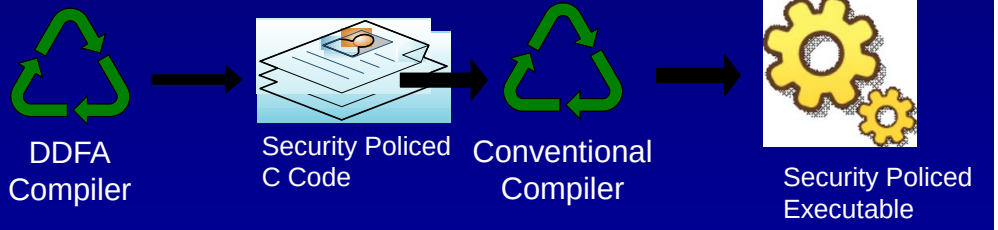


DDFA Runtime Library

Static dataflow analysis minimizes instrumentation

Policy and dynamic data flow analysis provide customized error mitigation





Need for Smart Grid Security R&D

- Ongoing threat & risk assessment of new SG devices
- Enhanced decapping protections for TPM modules
- Increased RD&T for open source, TCG stack
- Enhancements to the DDFA compiler
- Support for more languages within the DDFA compiler
- Addition of new DDFA “fight through attack” policies

Questions and Answers

Proceedings of the 17th Symposium for
Improving Building Systems
in Hot and Humid Climates
Austin Texas
August 24-25, 2010